DEFECT DETECTION AND PREVENTION

Steven L. Cornford, Jet Propulsion Laboratory, California Institute of Technology

BIOGRAPHY

Dr. Cornford graduated from U.C. Berkeley with B. S. degrees in Mathematics and Physics in 1984. He received his M. S. and Ph. D. in Physics from Texas A&M University in 1988 and 1992, respectively. He is currently a Technical Group Supervisor of the Reliability Technology Group at the Jet Propulsion Laboratory where he is managing the R&D efforts in Reliability Assurance. These efforts currently include: Advanced Technology Qualification, Flight Performance Evaluations, Flight Anomaly Characterizations, Test Effectiveness Experiments and Evaluations, Advanced Verification Methods Development and Implementation, Technical Risk Assessments and Management, Guidelines and Standard Development and Product Assurance Program Assessments.

ABSTRACT

As NASA continues to implement its Faster, Better, Cheaper philosophy, new approaches for implementing Mission Assurance activities are being developed. Defect Detection and Prevention is a system-level methodology for identifying, assessing and mitigating risk. Requirements are evolved through an iterative process which also identifies the occurrences of failure modes which could preclude a requirement being met. This approach first weights the relevant failure mocks against these requirements (functional, environmental, operational, etc.). These weighted failure modes are then weighted by the ability of a PACT (Preventative measure, Analyses, process Control or Test) to prevent or detect these failure modes. The combined weighted sums yield information which can be used to identify combinations of PACTS, perform the associated cost/risk tradeoffs, and ensure. resources are focused on "tall poles". The objective of this methodology is to achieve Better spacecraft while simultaneously building them Faster and Cheaper.

KEYWORDS

Hardware Qualification, QFD, Physics of Failure, Failure Modes, Defect Detection, Defect Prevention, Test Effectiveness, Screening, Risk Management, Mission Assurance, Reliability

INTRODUCTION

As NASA enters the new Millennium, the thrust towards building Faster, Better, Cheaper (FBC) spacecraft is well underway. There are a variety of forces driving NASA to this approach including: 1) decreasing budgets, 2) undesirability of "putting all the science eggs in one mission basket" which results in a small number of highly expensive spacecraft which then "can't fail", 3) a desire to infuse advanced technologies into space missions, and 4) a very large marginal cost savings for small decreases in reliability even without innovation, to name a few of the most obvious. The desire and need to develop FBC spacecraft is thus clear. The means of achieving Faster and Cheaper spacecraft are also clear: reduce funding and shorten developmental schedules, but to achieve Better will require a significant paradigm shift. The methods by which high reliability has been ensured to date, (solving every identified problem to minimize risk with secondary attention to cost), will no longer be applicable. The concept of "risk as a resource'" must be utilized when trading off cost, schedule, performance and risk. This is not to say that we will be "risky" but rather we will be taking calculated risks. A methodology originally developed by the author and Phillip R. Barela at the Jet Propulsion Laboratory under funding from NASA, Code Q (Office of Safety & Mission Assurance), has been implemented to meet this need to identify risk and provide the tools necessary to perform the cost/risk tradeoffs and facilitate the shift in assurance paradigms.

APPROACH

The methodology by which informed resource tradeoff decisions (remember risk is a resource!) are made is entitled: Defect, Detention and Prevention (DDP). This title is to be interpreted in the broadest sense of the words: Defects are those caused at any stage in the design, fabrication/assembly and integration processes; Preventions may include initial design rules, planned workarounds, functional redundancy, and materials and parts selection through redesign. **Figure** 1 is a conceptual diagram illustrating that all of these activities are on equal footing when considered as "screens" which prevent failure modes from reaching the mission. In this paper, I will use "screen" in its literal sense - screens keep failure modes from falling into the hardware undetected. These Detection and Prevention activities are abbreviated as PACTS (Preventions, Analyses, Process Controls and Tests) and none are considered sacred: the methodology evaluates all of these activities on a cost/benefit basis. For example, a combination of materials selections, process controls and functional testing may be more cost effective at finding the failure modes of concern than inspections, analyses and thermal vacuum testing. It is also possible that the opposite is true. The heart of the DDP methodology is providing the information necessary to make these cost/risk tradeoffs. Given limited project resources (dollars and

schedule), it is imperative to focus attention on the "tallest poles" and continue until a balance between available resources and acceptable risk has been achieved. While this is not a difficult concept to grasp, until now a methodology and tool-kit to achieve this derived state was not available. This methodology was initially developed in an attempt to qualify new, unproven technologies[2] but has recently been expanded to apply to spacecraft systems. The methodology may be applied to a number of JPL programs, but is utilizing the New Millennium Program (NM I') [3,4,5] as the pilot program.

Figure 1 may also be used to illustrate several other key points. Note that no box/activity/screen is 100% effective in screening all failure modes[1] and these "leakages" or "escapes" are denoted with dashed lines. This is an obvious point but is worth making because it illustrates why redundancies in assurance acti vities have evolved to where they are today in the ultra-low volume, high reliability spacecraft world: design it with redundancy and well documented design rules, double check the design, fabricate it with tight controls, inspect it at all levels of assembly, test it at all levels of assembly, document everything and still pray a lot after deployment. The fact that spacecraft failures exist today is evidence that even this expensive, brute-force, "shotgun" approach to ensure success is still not pet-fc.et, A big part of achieving faster and cheaper is to reduce the overlaps or redundancies between assurance activities.

However, as onc reduces the scope of assurance activities cm the.sc faster and cheaper missions, one wants to avoid "holes", or failure modes which fall through the screening process undiscovered until flight. To ensure optimization of rcsourccs, these failure modes must also bc weighted by ex tent of impact and likelihood of occurrence before deciding whether or not to take action.

The ACEQ (Accurate, Cost Effective Qualification) process (Reference 2) ut i lizes concurrent engineering bet wccn designers, system engineers and reliability engineers (and others as necessary) to develop two matl-ices: the Requirements matrix (RM) and the Effectiveness Matrix (EM) (illustrated in **Figure** 2). The KM plots failure modes (generated via a fault tree or "fishbone diagram" process) versus the requirements (mission, performance, lifetime, etc.) and weights the interactions with a O, 1, 3 or 9 depending on the criticality of the failure impact (higher numbers signify more impact). This completed RM yields valuable information regarding the general criticality of a failure mode (hits many requirements), the insignificance: of failure modes (hits no requirements) and the criticality or insignificance of individual requirements.

The EM plots these same failure modes versus the I'AC'I's (or mitigation activities) which can be performed. Both the cost of each activity and the relative effectiveness of these screens (at preventing or detecting these failure modes) are captured in this matrix. Again, the interactions are weighted with a O, 1, 3 or 9, but now as a metric regarding effectiveness. However, the failure modes arc also weighted by their criticality on, and likelihood of, impacting the requirements. This weighted sum is captured on the EM and allows one to focus on those failures modes of greatest concern (higher numbers significantly greater effectiveness). The EM then provides information regarding undetected o r over-dctceteci fail ure rnodcs (redundancy between PACT activities) and cost effective combinations of PACTS. The completed matrix may thus bc utilized to assess the combination of PACTS which best address the relevant risks within the available resources. This basic methodology is at the heart of the Defect Detection anti Prevention approach.

DEFECT DETECTION AND PREVENTION PROCESS

DDP is an iterative process performed as a natural (or concurrent) part of the requirements development and implementation process. **Figure 3** illustrates the most important elements of DDP:

1 Requirements Generation
The initial set of requirements which starts the process (mission and space, objectives, environment, etc.) are denoted "fundamental". At some point, a design tradeoff or technology selection results in additional lower level requirements which arc denoted "derived". It is these derived requirements which must be tracked and monitored for applicabilit y and useful ness.

2) Failure Mode Identification
Figure 4 illustrates the iterative nature of the requirements and failure mode development process. In this figure, requirements are denoted as horizontal lines, while failure modes are denoted as vertical lines. Note that each requirement leads to a new set of failure modes (or things which could keep the requirements from being met).

3) PACT identification
At this point, the PACT Effectiveness versus the identified failure modes is generated. This PACT

[1] The term "Failure Modes" is intended to cover both "hard" (cracks, explosions, complete shutdown, etc.) and "soft" failures (resets performance degradations, out of specificat ion performance, etc.).

list represents corporate culture and is updated as new methods and techniques become available.

4) PACT Refinement
'I'he weighted sum of the RM and EM is now utilized to select among available PACTs to assess adequacy and cost effectiveness. In cases where PACTS had uncertain effectiveness, alternatives can be chosen or focused efforts to evaluate this specific effectiveness can be performed.

5) Requirements Implementation
The requirements generated through this process arc then implemented in the hardware development process. As this process proceeds, new or different derived requirements arc generated which feeds back to the first step.

These five steps arc repeated until launch (and possibly into the mission itself), although the number of changes resulting from the iterations reduces as the hardware design matures. In the early stages of development, DDP is primarily utilized to shape the Mission Assurance program including: Design Philosophy, Test Program, Reliability and Quality Assurance Program, Functional Redundancies, etc. In the later stages of the development, DDP is utilized to tailor the integration and test program as issues arise. The DDP process is pm-titularly useful at this later stage, as one can quickly and effectively weight the impact and likelihood of a particular failure mode on the existing project requirements by the cost and relative effectiveness of various available mitigation activities (redesign, life test, etc.). A decision can then be made regarding the necessity of performing the various risk mitigation options. Sometimes, one will just save the money and choose to accept the. risk.

K} :QUIREMENTS MATKJX DEVELOPMENT

As the requirements develop, it is a natural part of the design process to identify potential problem areas which may impact the ability to achieve these requirements. S teps are t hen taken to prevent the occurrence of these failure modes through the design process itself (robust design, planned workarounds, block or functional materials selection, redundancy, etc.). In addition, activities are identified to detect failure modes (either design or workmanship) which remain in the hardware (Built in Self test, Process Controls, Functional Testing, Environmental Testing, Environmental Stress Screening, etc.). Traditionally, onc performs the best design possible and then "double checks" everything through a variety of testing. In the I DDP approach, the design is focused on achieving only applicable fundamental and derived requirements. Subsequent verification is only performed when the uncertainty in the preventative measures is great enough or when a mode could not be designed away and must be specifically checked as to whether it is present or not.

The DDP process also provides a vehicle for documenting the identified failure modes (and their associated criticality and probability of occurrence) by mapping the failure modes against the requirements to date. As project decisions arc made, some of the recommended mitigation activities may coalesce into requirements. These requirements will result in ncw failure modes and so on. The point of this part of the process is to weight the failure modes' impact on evolving requirements. Of particular concern are requirements (which arose as a response to an identified failure mode) which introduce ncw failure modes. For example, to ensure appropriate enci-of-life performance, an elevated temperature test may look like a viable option and thus a requirement, but another hardware constituent may be unacceptably degraded by this elevated temperature. In this example, another choice would be made (Voltage Margin lest, Worst Cast Analysis, etc.) to achieve the original objectives without exciting the temperature degradation failure mode. The systematic, iterative process described above ensures:

1) Failure modes arc identified

2) Failure Modes arc weighted by likelihood of occurrence anti impact on mission requirements.

3) Ncw requirements are captured (as wel 1 as the reasons for becoming a requirement -- which failure modes it is being added to prevent or detect). Note that if the hardware or failure modes change, the justification for requiring various PACT activities (and incurring their associated cost and schedule hits) may disappear.

4) The focus is on physics of fail ure (underlying cause) and those failure modes which directly impact the identified mission requirements. In today's environment of Faster, Better and Cheaper, wc must focus our resources on solving the problems which arc of the most concern to our project.

I EFFECTIVENESS MATRIX DEVELOPMENT

These identified and weighted failure modes are then mapped against the available PACT's (Preventative measures, Analysis, process Controls and Tests). The effectiveness of these activities at preventing or detecting these failure modes is entered into the EM. This

information may be available from corporate experience, available literature, applied research, fundamental physics or engineering judgement. An important part of the corporate infrastructure which enables these effectiveness entries is the evaluation of the effectiveness of the activities performed on previous spacecraft or hardware projects. It is assumed that the implementation of continuous improvement techniques have already resulted in internal evaluations of the cost benefit of various "essential" processes.

In cases where the effectiveness of a given activity is unknown, a symbol (e.g. "*") may be entered into the FM. 1 f another selected PACT is found to be effective at screening for this failure mode, the "*" becomes irrelevant, If this PACT appears to be the only hope of screening for a failure mode of concern, focused efforts may then be performed to ascertain the effectiveness. However, another option is to just "accept the risk" and move on.

SUMMARY

1 t is presentl y the intent of the DDP process to provide concurrent identification of failure modes and identify tni tigat ion options (PACTS) which detect or prevent the failure mode occurrence. This allows project managers to intelligently select the combinations of PACTs which meet their resources and risk posture. The goal of the DDP methodology is to achieve the Better part of the NASA Faster, Better, Cheaper paradigm while remaining sensitive to the I 'aster anti Cheaper parts. The Defect Detection and Prevention methodology has been described. It utilizes a physics of failure (underlying cause) approach to focus tbc design and requirement generation process to the minimum necessary to achieve the desired mission objectives. Tbe failure modes (or ways a requirement won' t be met) are weighted by the severity and likelihood of occurrence. These failure modes arc then mapped against available mitigation activities, or PACTs, and the effectiveness at detecting or preventing failure modes of concern is assessed. This weighted effectiveness matrix is then used to develop an assurance program within resource constraints. This iterative process is updated as the requirements, failure modes and hardware changes to ensure that all PACTs and requirements arc relevant and value-added. This allows "real time" cost/risk tradeoffs to be made as problems arise.

The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology under a contract with the National Aeronautics and Space Administration through Code Q.

REFERENCES

↳ to top of next column.

[1] Gindorf, T. E. and Greenfield, M., *Risk as a Resource -- A New Paradigm*; International Conference on Probabilistic Safety Assessment and Management; June 24-28, 1996, Crete, Greece

[2] Cornford, S. L. and Barela, P. R., *A Systematic Approach to Hardware Qualification*, 1 f :SATM Proceedings, May 1995, Anaheim, CA

[3] Ridenoure, R. W., *Key Architectural issues and Trade-offs for the New Millenn ium Advanced Technology Validation Missions,* Proceedings for tbc 34th A l A A Aerospace Sciences Conference and Exhibit, Jan 1996

[4] Casani, E. K., Wilson, B. W. and Ridenoure, R. W.; The New *Millennium Program: Positioning NASA for Ambitious Space and Earth Science Missions for the 21st Century;* Paper and presentation for the special session on future space and Earth sciences missions at the Space Technology and Applications International Forum (SI'AIF-96), 1996 January 7-11, Albuquerque, NM.

[5] Casani, E. K. and Wilson, B. W.; *The* New *Millennium Program: Technology Development for the 21st Century*; AIAA 34th Aerospace Sciences Meeting and Exhibit, January 171996, Reno, NV, Paper #AlAA 96-0696

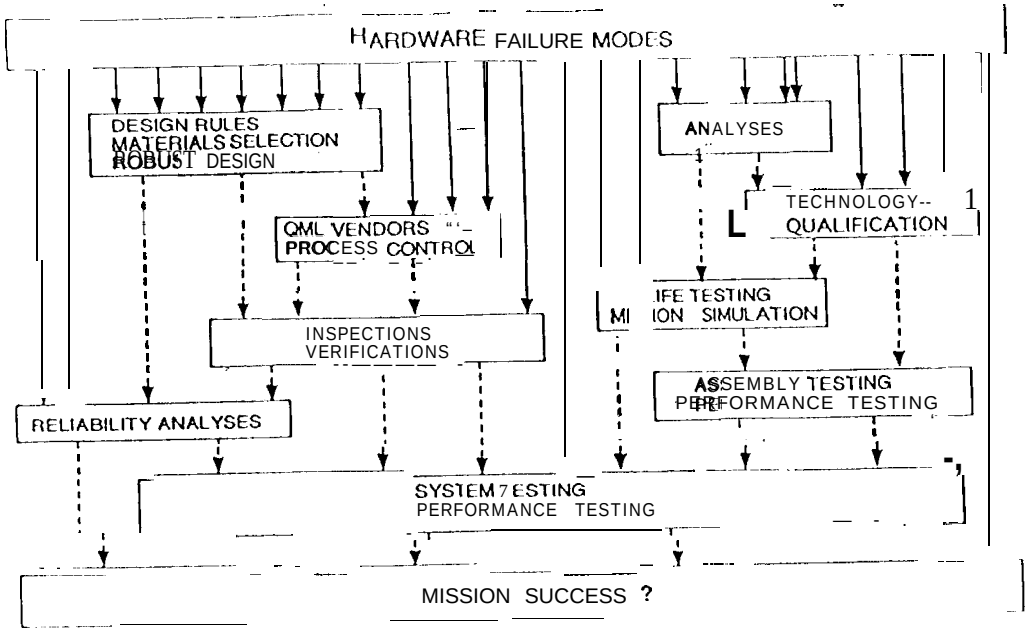

Figure 1: An illustration of the activities (or PACTs) which are normally performed to ensure detection or prevention of failure modes which could adversely impact mission objectives.

Requirements Matrix (RM)

	DERIVED FAILURE MODES						
	9	1	3	1	3		
REQUIREMENTS				1	9	1	SUM YIELDS
(FUNDAMENTAL	3			3	9	1	REQUIREMENT
AND DERIVED)	3						DRIVER
	1	9	3	3		9	COEFFICIENTS
		1	1		3		
	9		3	3		3	
	SUM YIELDS WEIGHTED FAILURE MODE IMPACT COEFFICIENTS						

Effectiveness Matrix (EM)

	WEIGHTED FAILURE MODES						
	3	9	9		3		
PACTs				1	1	1	WEIGHTED
(Preventions,	3			3	1	1	COST
Analyses, process	3				3		EFFECTIVENESS
Controls and Tests)		3		1	9	9	FOR IDENTIFICATION
	3	3	3		1		AND MITIGATION
	1	9		9		1	
	SUM YIELDS DEGREE TO WHICH FAILURE MODE IS DETECTED/PREVENTED						

Figure 2: An illustration of the two matrices at the heart of the DDP process: the Requirements Matrix (RM) and the Effectiveness Matrix (EM).

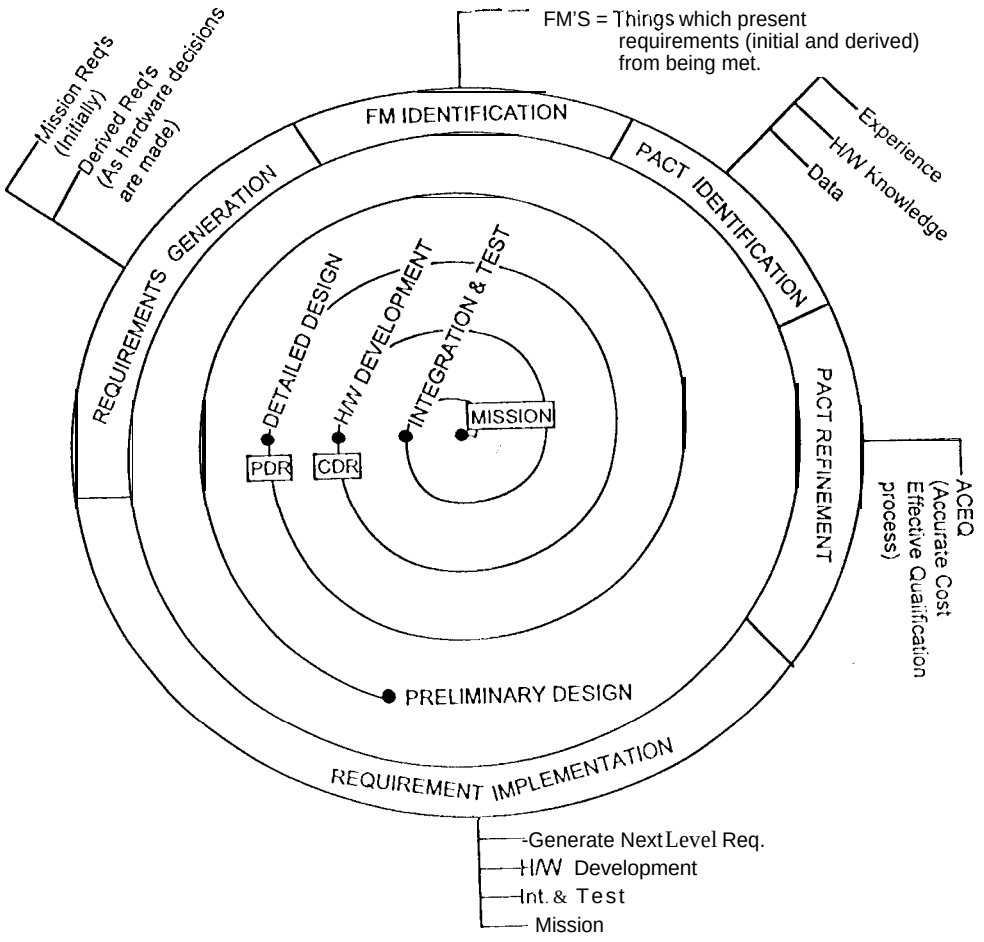

Figure 3: An illustration of the iterative process of Requirements Generation to Requirements Implementation.

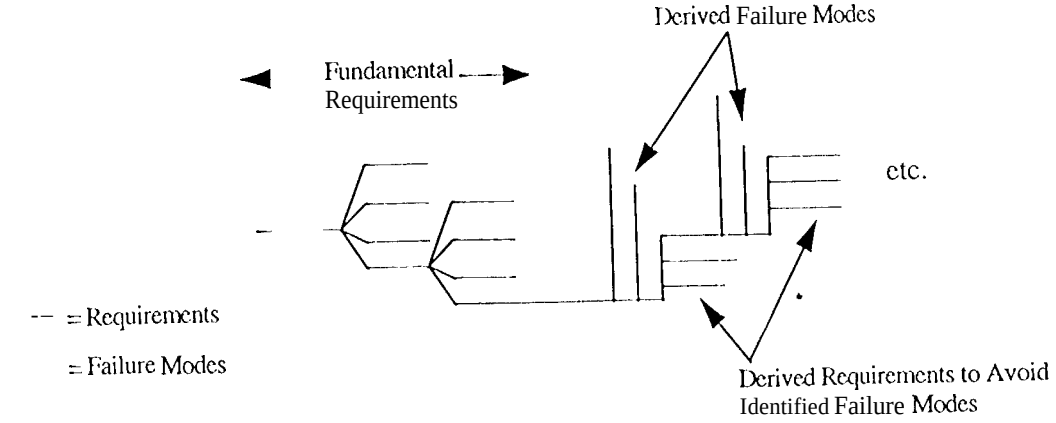

Figure 4: An illustration of the Requirements Generation process.